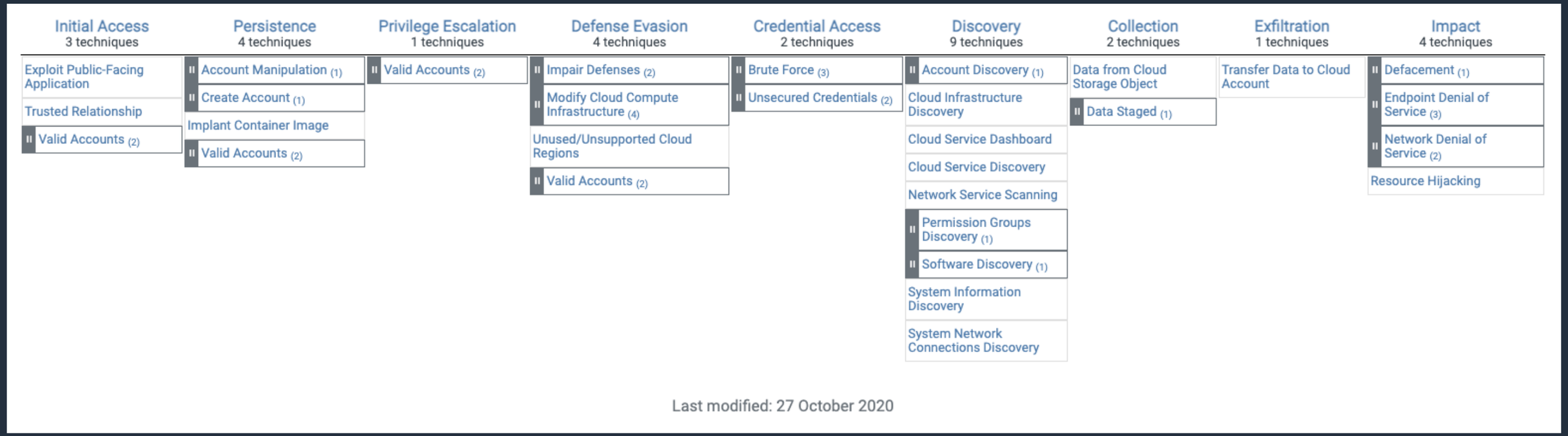
亚马逊云科技

2021 Security Day

探测与防护控制

云上的威胁： MITRE ATT&CK –Metrix

以下是代表面向云技术的MITRE attack & ck®矩阵的战术和技术。该矩阵包含AWS平台的信息。



OWASP Top 10

OWASP Top 10是一个针对开发人员和web应用安全的标准文档。它代表了关于web应用程序最关键的安全风险的广泛共识。

注入	将不受信任的数据作为命令或查询的一部分发送到解析器时，会产生诸如SQL注入、NoSQL注入、OS 注入和LDAP注入的注入缺陷。攻击者的恶意数据可以诱使解析器在没有适当授权的情况下执行非预 期命令或访问数据。
失效的身份认证	通常，通过错误使用应用程序的身份认证和会话管理功能，攻击者能够破译密码、密钥或会话令牌， 或者利用其它开发缺陷来暂时性或永久性冒充其他用户的身份。
敏感信息泄露	许多Web应用程序和API都无法正确保护敏感数据，例如：财务数据、医疗数据和PII数据。攻击者可 以通过窃取或修改未加密的数据来实施信用卡诈骗、身份盗窃或其他犯罪行为。未加密的敏感数据 容易受到破坏，因此，我们需要对敏感数据加密，这些数据包括：传输过程中的数据、存储的数据 以及浏览器的交互数据。
XML 外部实体（XXE）	许多较早的或配置错误的XML处理器评估了XML文件中的外部实体引用。攻击者可以利用外部实体窃 取使用URI文件处理器的内部文件和共享文件、监听内部扫描端口、执行远程代码和实施拒绝服务攻 击。
失效的访问控制	未对通过身份验证的用户实施恰当的访问控制。攻击者可以利用这些缺陷访问未经授权的功能或数 据，例如：访问其他用户的帐户、查看敏感文件、修改其他用户的数据、更改访问权限等。
安全配置错误	安全配置错误是最常见的安全问题，这通常是由于不安全的默认配置、不完整的临时配置、开源云 存储、错误的 HTTP 标头配置以及包含敏感信息的详细错误信息所造成的。因此，我们不仅需要对所 有的操作系统、框架、库和应用程序进行安全配置，而且必须及时修补和升级它们。
跨站脚本（XSS）	当应用程序的新网页中包含不受信任的、未经恰当验证或转义的数据时，或者使用可以创建 HTML或 JavaScript 的浏览器 API 更新现有的网页时，就会出现 XSS 缺陷。XSS 让攻击者能够在受害者的浏览器 中执行脚本，并劫持用户会话、破坏网站或将用户重定向到恶意站点。
不安全的反序列化	不安全的反序列化会导致远程代码执行。即使反序列化缺陷不会导致远程代码执行，攻击者也可以 利用它们来执行攻击，包括：重播攻击、注入攻击和特权升级攻击。
使用含有已知漏洞的组件	组件（例如：库、框架和其他软件模块）拥有和应用程序相同的权限。如果应用程序中含有已知漏 洞的组件被攻击者利用，可能会造成严重的数据丢失或服务器接管。同时，使用含有已知漏洞的组 件的应用程序和API可能会破坏应用程序防御、造成各种攻击并产生严重影响。
不足的日志记录和监控	不足的日志记录和监控，以及事件响应缺失或无效的集成，使攻击者能够进一步攻击系统、保持持 续性或转向更多系统，以及篡改、提取或销毁数据。大多数缺陷研究显示，缺陷被检测出的时间超 过200天，且通常通过外部检测方检测，而不是通过内部流程或监控检测。

Center for Internet Security (CIS) Amazon Web Services Foundations

CIS安全基准程序提供了定义明确、公正、基于共识的行业最佳实践，以帮助组织评估和提高其安全性。亚马逊云科技是CIS安全基准测试的成员公司

	Control	Set Correctly	
		Yes	No
1	**Identity and Access Management**		
1.1	Avoid the use of the "root" account (Scored)	☐	☐
1.2	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)	☐	☐
1.3	Ensure credentials unused for 90 days or greater are disabled (Scored)	☐	☐
1.4	Ensure access keys are rotated every 90 days or less (Scored)	☐	☐
1.5	Ensure IAM password policy requires at least one uppercase letter (Scored)	☐	☐
1.6	Ensure IAM password policy require at least one lowercase letter (Scored)	☐	☐
1.7	Ensure IAM password policy require at least one symbol (Scored)	☐	☐
1.8	Ensure IAM password policy require at least one number (Scored)	☐	☐
1.9	Ensure IAM password policy requires minimum length of 14 or greater (Scored)	☐	☐
1.10	Ensure IAM password policy prevents password reuse (Scored)	☐	☐
1.11	Ensure IAM password policy expires passwords within 90 days or less (Scored)	☐	☐
1.12	Ensure no root account access key exists (Scored)	☐	☐
1.13	Ensure MFA is enabled for the "root" account (Scored)	☐	☐
1.14	Ensure hardware MFA is enabled for the "root" account (Scored)	☐	☐
1.15	Ensure security questions are registered in the AWS account (Not Scored)	☐	☐
1.16	Ensure IAM policies are attached only to groups or roles (Scored)	☐	☐
1.17	Maintain current contact details (Not Scored)	☐	☐
1.18	Ensure security contact information is registered (Not Scored)	☐	☐
1.19	Ensure IAM instance roles are used for AWS resource access from instances (Not Scored)	☐	☐
1.20	Ensure a support role has been created to manage incidents with AWS Support (Scored)	☐	☐
1.21	Do not setup access keys during initial user setup for all IAM users that have a console password (Not Scored)	☐	☐
1.22	Ensure IAM policies that allow full "*:*" administrative privileges are not created (Scored)	☐	☐
2	**Logging**		
2.1	Ensure CloudTrail is enabled in all regions (Scored)	☐	☐
2.2	Ensure CloudTrail log file validation is enabled (Scored)	☐	☐
2.3	Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible (Scored)	☐	☐
2.4	Ensure CloudTrail trails are integrated with CloudWatch Logs (Scored)	☐	☐
2.5	Ensure AWS Config is enabled in all regions (Scored)	☐	☐
2.6	Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket (Scored)	☐	☐
2.7	Ensure CloudTrail logs are encrypted at rest using KMS CMKs (Scored)	☐	☐
2.8	Ensure rotation for customer created CMKs is enabled (Scored)	☐	☐
2.9	Ensure VPC flow logging is enabled in all VPCs (Scored)	☐	☐
3	**Monitoring**		
3.1	Ensure a log metric filter and alarm exist for unauthorized API calls (Scored)	☐	☐
3.2	Ensure a log metric filter and alarm exist for Management Console sign-in without MFA (Scored)	☐	☐
3.3	Ensure a log metric filter and alarm exist for usage of "root" account (Scored)	☐	☐
3.4	Ensure a log metric filter and alarm exist for IAM policy changes (Scored)	☐	☐
3.5	Ensure a log metric filter and alarm exist for CloudTrail configuration changes (Scored)	☐	☐
3.6	Ensure a log metric filter and alarm exist for AWS Management Console authentication failures (Scored)	☐	☐
3.7	Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs (Scored)	☐	☐
3.8	Ensure a log metric filter and alarm exist for S3 bucket policy changes (Scored)	☐	☐
3.9	Ensure a log metric filter and alarm exist for AWS Config configuration changes (Scored)	☐	☐
3.10	Ensure a log metric filter and alarm exist for security group changes (Scored)	☐	☐
3.11	Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL) (Scored)	☐	☐
3.12	Ensure a log metric filter and alarm exist for changes to network gateways (Scored)	☐	☐
3.13	Ensure a log metric filter and alarm exist for route table changes (Scored)	☐	☐
3.14	Ensure a log metric filter and alarm exist for VPC changes (Scored)	☐	☐
4	**Networking**		
4.1	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22 (Scored)	☐	☐
4.2	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389 (Scored)	☐	☐
4.3	Ensure the default security group of every VPC restricts all traffic (Scored)	☐	☐
4.4	Ensure routing tables for VPC peering are "least access" (Not Scored)	☐	☐

亚马逊云科技

为什么需要探测控制?

- 预防性控制并非万灵药
- 发现使反应
- 最小特权很难实现，也更难维护
- 坏人总是在寻找新的方法来规避控制
- 监管机构和审计机构需要证据
- 简化调试和维护性能
- 提高开发人员的生产力并鼓励创新

主要的安全需求

安全监控与威胁检测

数据保护

保护范围

Amazon EC2

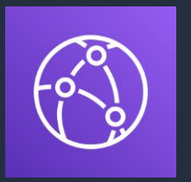
AWS Identity and Access Management (IAM)

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (S3)

Amazon EC2

Elastic Load Balancing (ELB)



Amazon CloudFront

安全监控与威胁检测

安全监控与威胁检测

Amazon EC2

AWS Identity and Access Management (IAM)

Amazon Simple Storage Service (S3)

Amazon GuardDuty

Amazon Inspector

Amazon Macie

AWS Security Hub

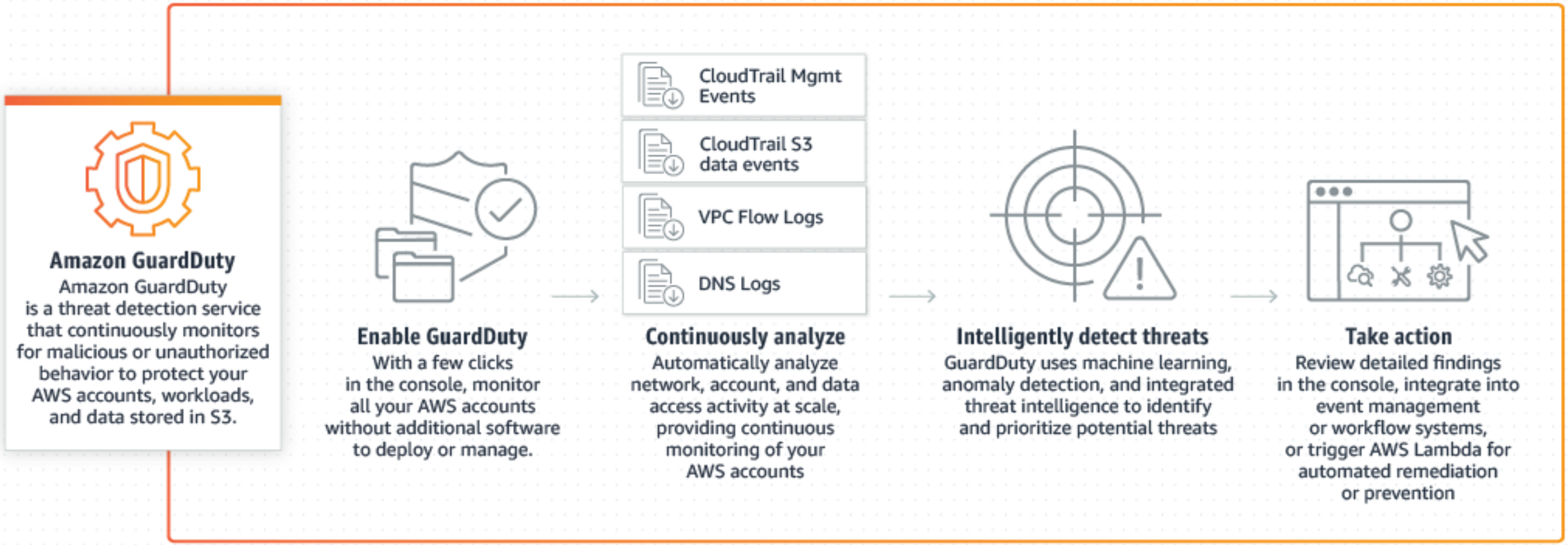
Amazon Detective

“采取行动”

亚马逊云科技

托管的威胁检测服务 GuardDuty?

通过智能威胁检测和持续监控保护您的AWS帐户和工作负载



威胁检测服务GuardDuty怎么工作?

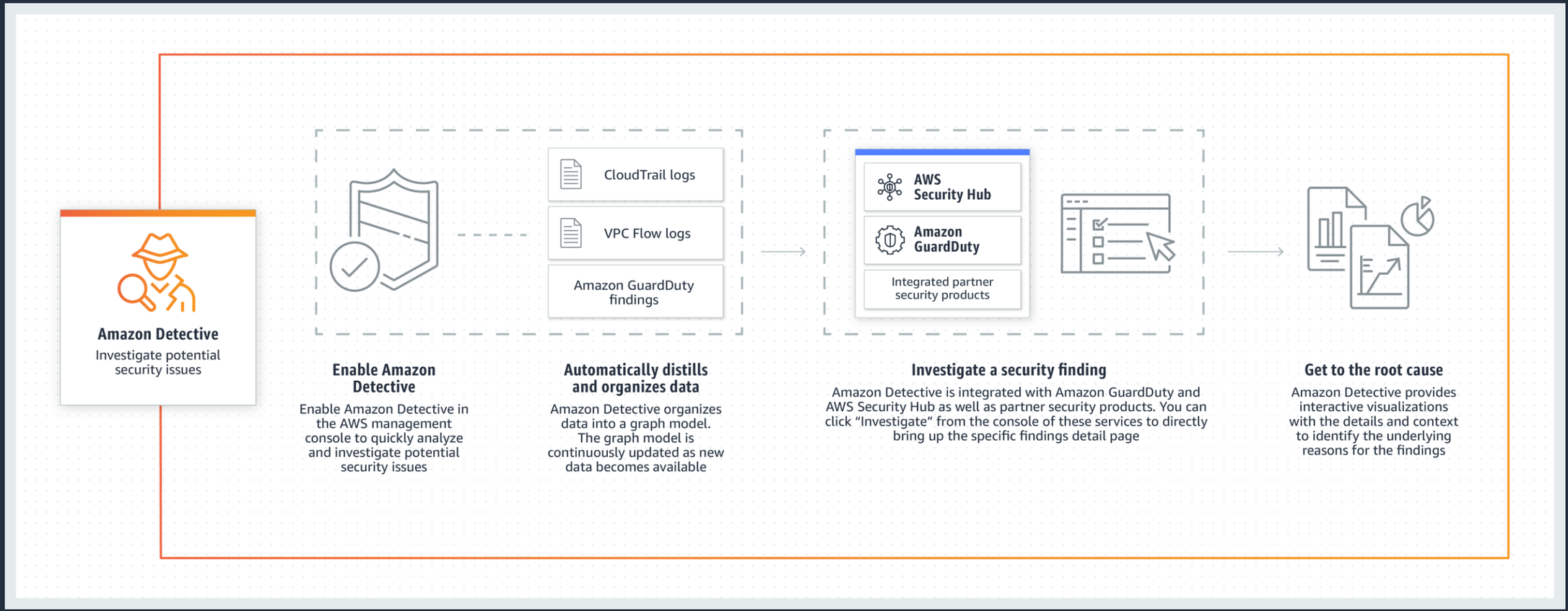
威胁检测服务 GuardDuty 可以发现什么?

超过50种，并在不断增长中…

- Backdoor Finding Types
- Behavior Finding Types
- Crypto Currency Finding Types
- PenTest Finding Types
- Persistence Finding Types
- Policy Finding Types
- Privilege Escalation Finding Types
- Recon Finding Types
- Resource Consumption Finding Types
- Stealth Finding Types
- Trojan Finding Types
- Unauthorized Finding Types

什么是Detective

Amazon Detective自动从您的AWS资源收集日志数据，并使用机器学习、统计分析和图理论来构建一组链接数据，使您能够轻松地进行更快、更有效的安全调查。借助该服务，安全团队能够轻松地调查并快速找到发现的安全问题或可疑活动根本原因。Amazon Detective可以分析来自多个数据源的数万亿事件，如VPC流日志、AWS CloudTrail、Amazon GuardDuty等，并自动创建一个统一的、交互式的资源、用户以及他们之间的交互视图。有了这个统一的视图，您可以在一个地方可视化所有的细节和上下文，以确定发现结果的潜在原因，深入到相关的历史活动中，并快速确定根本原因。



Amazon Detective使用场景

分类安全检测结果

多少数据发送出去?
网络流量正常吗?
刚才发生了什么?
这些失败调用正常吗?

事故调查

从这个ip发出了什么API调用?
这些访问是否表明有探测?
还有其他的主题ID被使用了?
还有其他EC2和这个ip通信吗?

威胁搜寻

威胁报告里的ip地址在去年和那些ec2实例通信了?
这个可疑的用户的代理访问了哪些API调用?

现在的状态

Observed EC2 instances using this IP address Info

Lorem ipsum dolor amet intelligentsia subway tile single-origin coffee tote bag. Gluten-free enamel pin ennui migas blog williamsburg street art humblebrag iceland mixtape roof party freegan before they sold out.

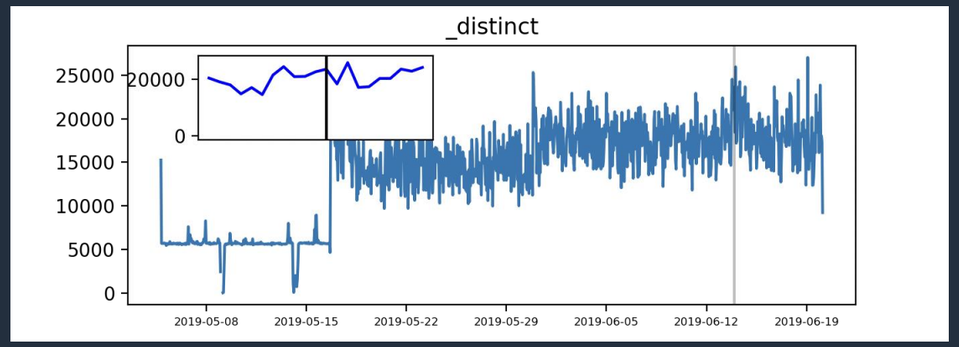
EC2 instance	First time observed	Last time observed
i-1234a5b678c901d23	11/10/18, 23:00	11/13/19, 14:00
i-4567d8e901f234g56	10/28/19, 15:00	11/12/19, 16:00

[Time series label]

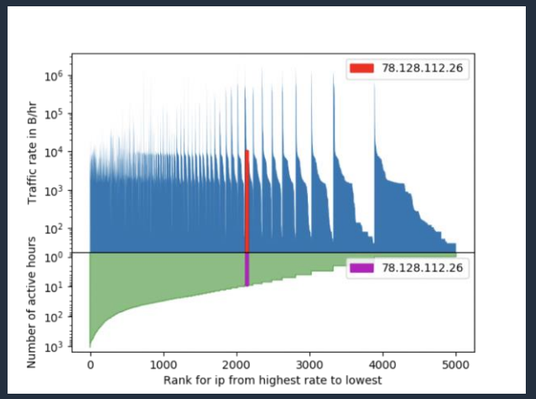
Scope: 10/18 @21:00 - 10/19 @23:00

i-7890h1j234k567l89	11/13/19, 13:00	11/13/19, 13:00

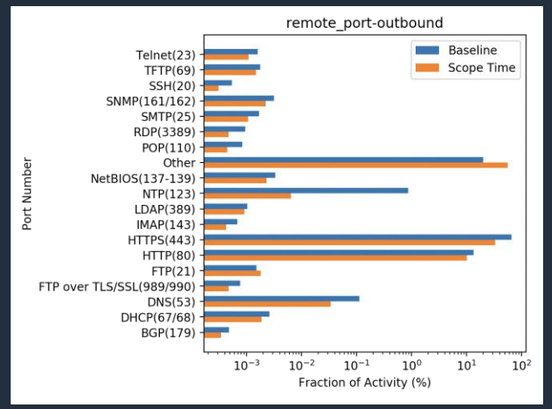
由数据科学家支持的分析结果



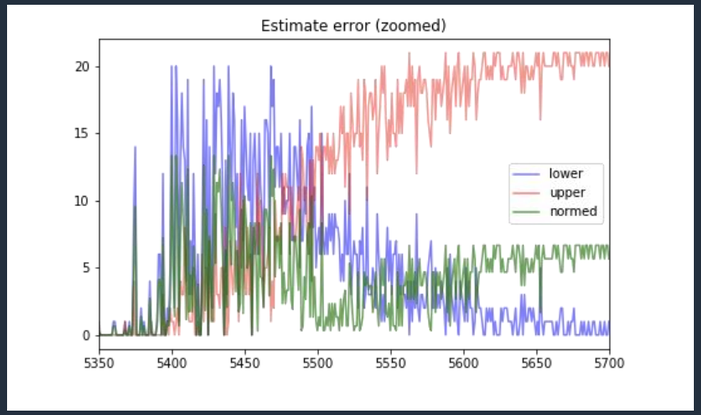
Behavioral baselines



Distributions



Time series analysis



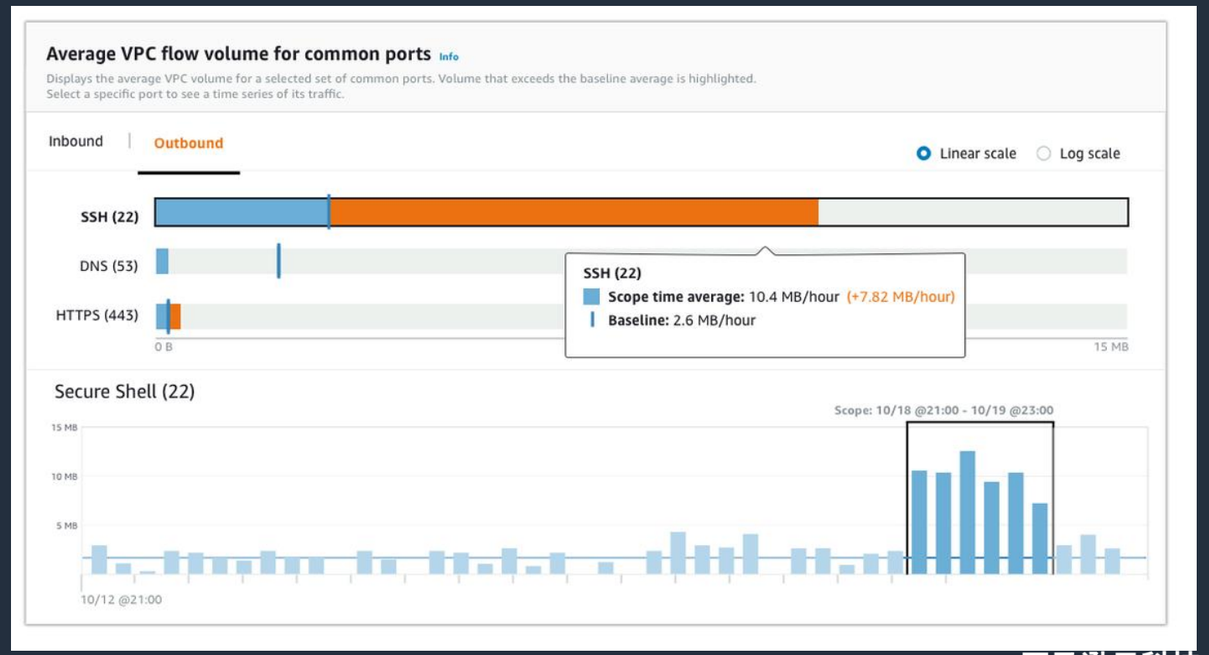
Data stream analytics

刚才发生了什么?

这些失败调用正常吗

发送了多少数据?

这个流量正常吗?



Inspector 对什么进行探测，进行什么评估?

网络可达性评估： Amazon Inspector 是一项自动安全评估服务，自动评估应用程序的风险、漏洞或者相较于最佳实践的偏差。执行评估后，Amazon Inspector 会生成按严重程度确定优先级的安全检测详细列表。这些评估结果可直接接受审核，也可作为通过 Amazon Inspector 控制台或 API 提供的详细评估报告的一部分接受审核。

Inspector 默认是无代理模式，客户可以选择安装代理，实现更细致的评估。

- 安全组
- vpc
- 网络接口
- 子网
- 网络ACL
- 路由表
- 弹性负载平衡器
- 应用程序负载平衡器
- 互联网网关
- 虚拟专用网关
- DX
- VPC对等连接

常见漏洞 (CVE)

Internet 安全中心 (CIS) 基准

安全最佳实践

运行时行为分析

Inspector 无代理模式下的发现示例

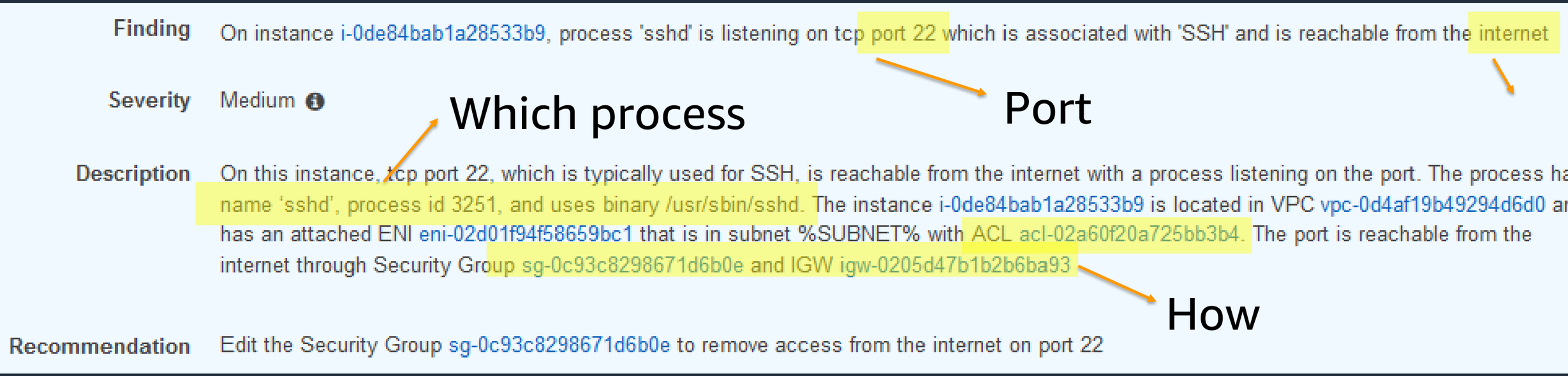
Finding	On instance i-0df739d0c3b0e1410, TCP port 22 which is associated with 'SSH' is reachable from the internet
Severity	Medium
Description	On this instance, TCP port 22, which is associated with SSH, is reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port. The instance i-0df739d0c3b0e1410 is located in VPC vpc-e6a88f9d and has an attached ENI eni-b59b2c2d which uses network ACL acl-56d85d2c. The port is reachable from the internet through Security Group sg-3fa76677 and IGW igw-f83d5680
Recommendation	Edit the Security Group sg-3fa76677 to remove access from the internet on port 22

Port

Where?

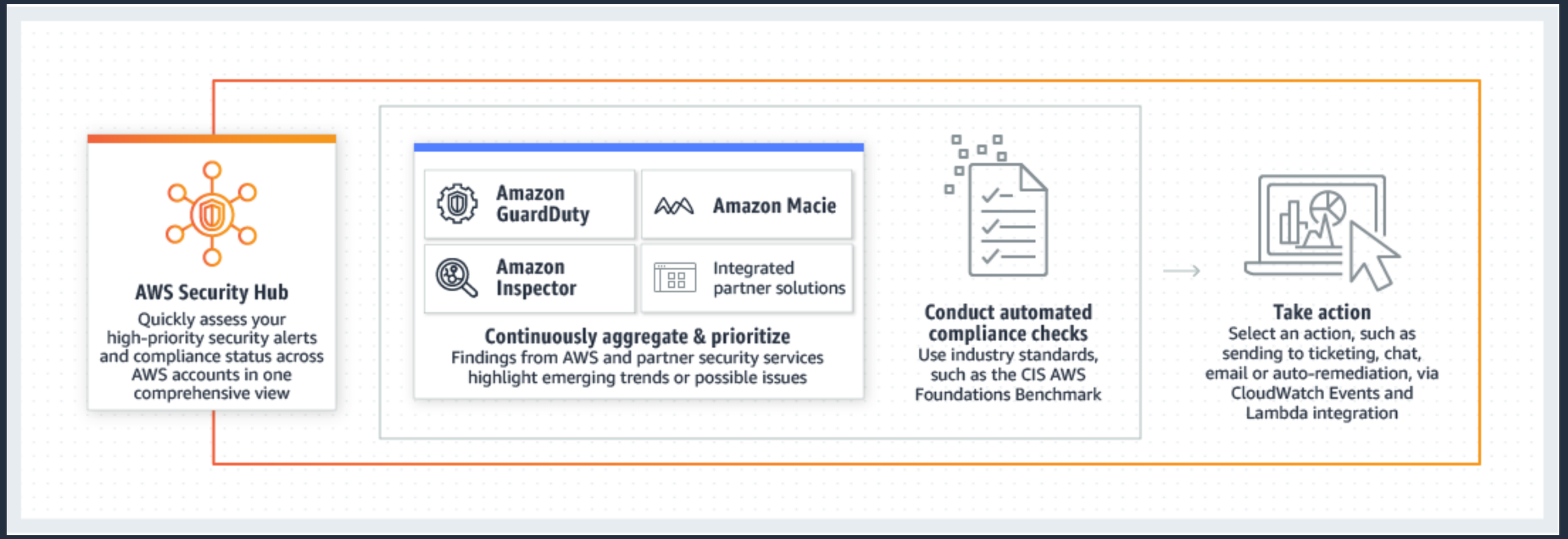
How?

Inspector 有代理模式下的发现示例（可选）

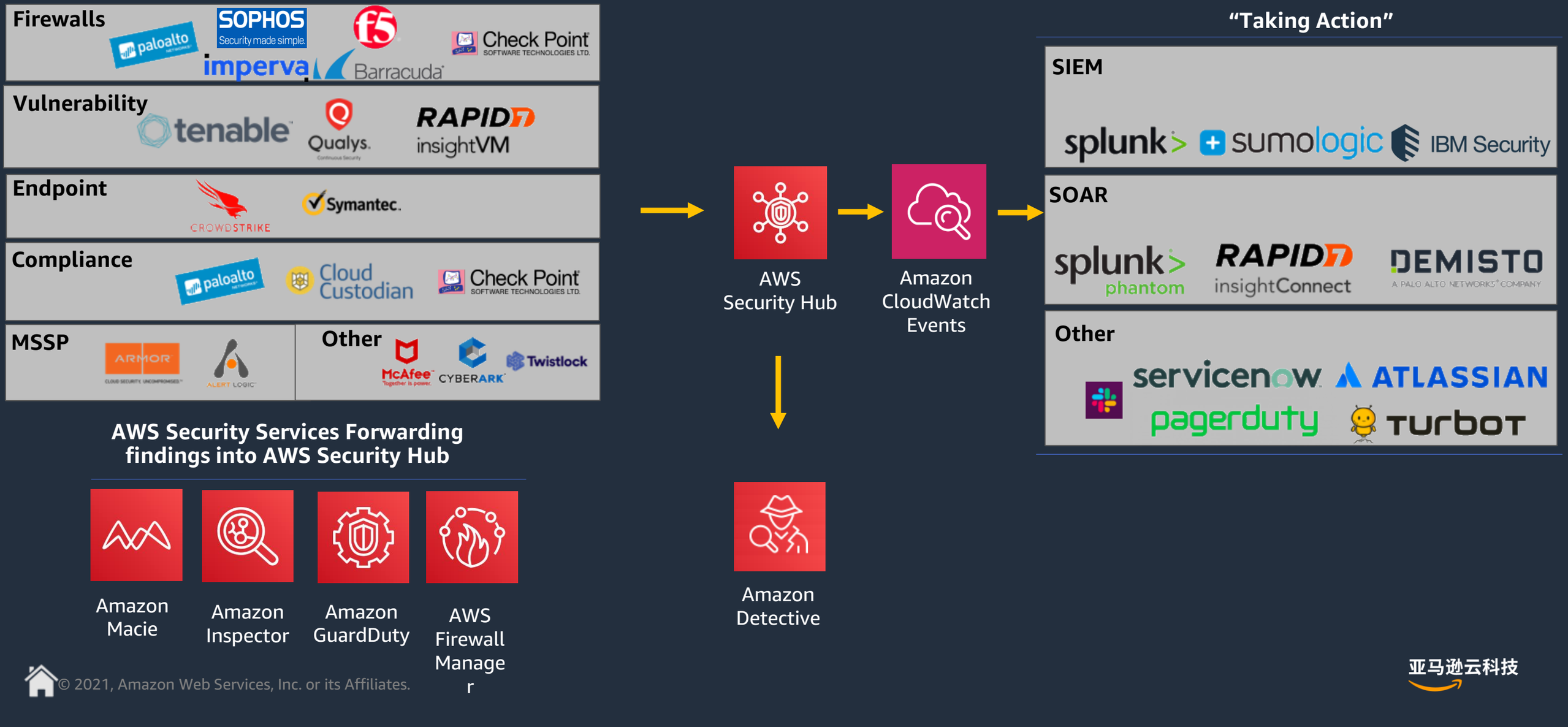


什么是 Security Hub

AWS Security Hub 可全面查看 AWS 账户中的高优先级安全警报与合规性状态。汇聚来自多个 AWS 服务（如 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie），以及来自 AWS 合作伙伴解决方案的安全警报或检测结果，设置优先级。图表展示。还可以使用自动合规性检查（基于您的组织遵守的 AWS 最佳实践和行业标准），持续监控您的环境。



Security Hub集成



Security Hub的使用场景

集中的安全和合规工作空间

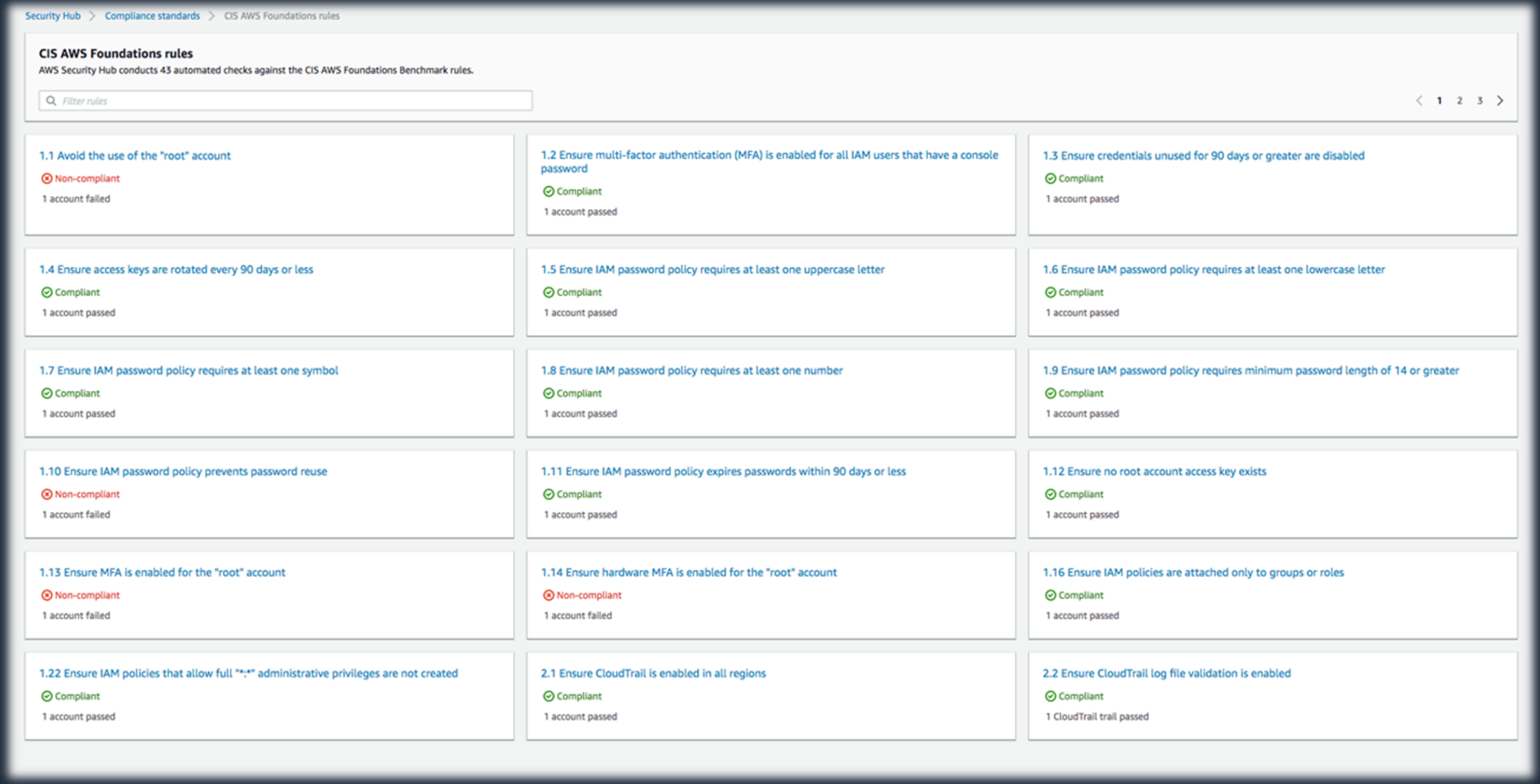
- 从数据源中获取发现
- 大量且知名的发现以编程方式路由到缓解工作流，其中包括更新发现的状态
- 剩下的调查结果通过一个随叫随到的管理系统传递给分析人员，他们使用工单或聊天系统来解决这些问题

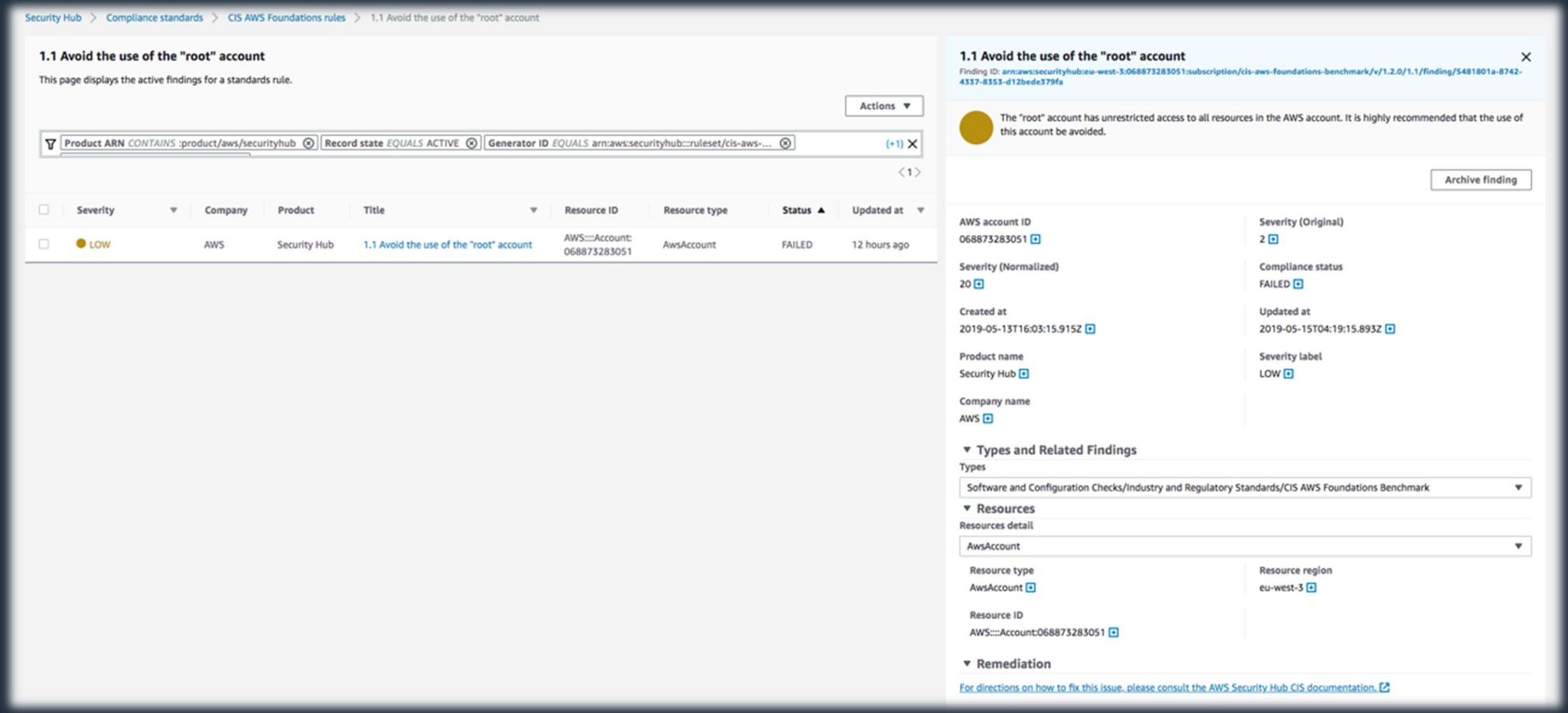
通向企业SIEM的集中路由

- 从数据源中获取发现
- 所有调查结果都将通过Amazon CloudWatch事件路由到存储AWS和内部安全与合规数据的中央SIEM
- 分析人员工作流程与中央SIEM相关联

账号负责人的仪表盘

- 从数据源中获取发现
- 帐户所有者被赋予对安全中心的只读访问权
- 帐户所有者可以使用Security Hub来研究他们所关注的问题，或主动监视自己的安全性和遵从性状态





安全服务和用户场景总结

安全监控和威胁检测

数据保护

保护范围

Amazon EC2

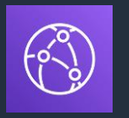
AWS Identity and Access Management (IAM)

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (S3)

Amazon EC2

Elastic Load Balancing (ELB)



Amazon CloudFront

Amazon GuardDuty

Amazon Inspector

AWS CloudHSM

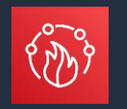
KMS

Amazon Macie

AWS Security Hub

“Take Action”

Amazon Detective



AWS Firewall Manager

AWS Shield Advanced

AWS WAF